
[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)

 Search: ☒ The ACM Digital Library ☐ The Guide


 Searching within **The ACM Digital Library** for: braid group digital signature ([start a new search](#))

 Found **8** of **268,156**

REFINE YOUR SEARCH

[Search Results](#)
[Related SIGs](#)
[Related Conferences](#)

Refine by
Keywords

[Discovered](#)
[Terms](#)

Refine by
People

[Names](#)
[Institutions](#)
[Authors](#)

Refine by
Publications

[Publication Year](#)
[Publication Names](#)
[ACM Publications](#)
[All Publications](#)
[Publishers](#)

Refine by
Conferences

[Sponsors](#)
[Events](#)
[Proceeding Series](#)

Results 1 - 8 of 8

 Sort by in
[Save results to a Binder](#)

1 [One-more matching conjugate problem and security of braid-based signatures](#)

[Licheng Wang, Zhenfu Cao, Peng Zeng, Xiangxue Li](#)

 March 2007 **ASI ACCS '07: Proceedings of the 2nd ACM symposium on Information, computer and communications security**
Publisher: ACM [Request Permissions](#)

 Full text available: Pdf (376.37 KB) [Additional Information: full citation, abstract, references, index terms](#)
Bibliometrics: Downloads (6 Weeks): 6, Downloads (12 Months): 49, Downloads (Overall): 210, Citation Count: 0

Braid groups have recently attracted the attention of many cryptographers as an alternative to number-theoretic public key cryptography. But the published braid-based signatures have failed to reach the most desired security, i.e., existential unforgeability ...

Keywords: braid-based signature, digital signatures, one-more matching conjugate problem, provable security

2 [Quantum resistant public key cryptography: a survey](#)

[Ray A. Perlner, David A. Cooper](#)

 April 2009 **IDtrust '09: Proceedings of the 8th Symposium on Identity and Trust on the Internet**
Publisher: ACM

 Full text available: Pdf (359.74 KB) [Additional Information: full citation, abstract, references, index terms](#)
Bibliometrics: Downloads (6 Weeks): 42, Downloads (12 Months): 230, Downloads (Overall): 230, Citation Count: 0

Public key cryptography is widely used to secure transactions over the Internet. However, advances in quantum computers threaten to undermine the security assumptions upon which currently used public key cryptographic algorithms are based. In this paper, ...

Keywords: public key cryptography, quantum computers

3 [Vulnerabilities of RFID systems in infant abduction protection and patient wander prevention](#)

[Mohamed K. Saad, Syed V. Ahamed](#)

 June 2007 **SI GCSE Bulletin**, Volume 39 Issue 2

Publisher: ACM

 Full text available: Pdf (148.47 KB) [Additional Information: full citation, abstract, references, index terms](#)
Bibliometrics: Downloads (6 Weeks): 15, Downloads (12 Months): 117, Downloads (Overall): 479, Citation Count: 0

This paper presents penetration attacks and abduction drills conducted in a healthcare facility relying on RFID security system to prevent infant abduction and patient wander. The objective is to provide a better understanding to the limitations and ...

Keywords: RFID, infant abduction, protection, vulnerabilities

ADVANCED SEARCH

[Advanced Search](#)

FEEDBACK

[Please provide us with feedback](#)

 Found **8** of **268,156**

4 [Determining the automorphism group of a hyperelliptic curve](#)



[Tanush Shaska](#)

August 2003 **ISSAC '03: Proceedings of the 2003 international symposium on Symbolic and algebraic computation**

Publisher: ACM [Request Permissions](#)

Full text available: [PDF](#) (250.89 KB)

[Additional Information: full citation, abstract, references, cited by, index terms](#)

Bibliometrics: Downloads (6 Weeks): 6, Downloads (12 Months): 30, Downloads (Overall): 286, Citation Count: 1

In this note we discuss techniques for determining the automorphism group of a genus g hyperelliptic curve X_g defined over an algebraically closed field k of characteristic zero. The first technique uses the classical $GL_2(k)$ -invariants of ...

Keywords: automorphism, hyperelliptic curve, moduli space

5 [Audio hallway: a virtual acoustic environment for browsing](#)



[Chris Schmandt](#)

November 1998 **UIST '98: Proceedings of the 11th annual ACM symposium on User interface software and technology**

Publisher: ACM [Request Permissions](#)

Full text available: [PDF](#) (65.62 KB)

[Additional Information: full citation, references, cited by, index terms](#)

Bibliometrics: Downloads (6 Weeks): 4, Downloads (12 Months): 35, Downloads (Overall): 424, Citation Count: 9

Keywords: auditory user interface, digitized speech, spatial audio, virtual environments

6 [Online pairing of VoIP conversations](#)

[Michail Vlachos](#), [Aris Anagnostopoulos](#), [Olivier Verscheure](#), [Philip S. Yu](#)

January 2009 **The VLDB Journal — The International Journal on Very Large Data Bases**, Volume 18 Issue 1

Publisher: Springer-Verlag New York, Inc.

Full text available: [PDF](#) (1.53 MB)

[Additional Information: full citation, abstract, references, index terms](#)

Bibliometrics: Downloads (6 Weeks): 16, Downloads (12 Months): 89, Downloads (Overall): 89, Citation Count: 0

This paper answers the following question; given a multiplicity of evolving 1-way conversations, can a machine or an algorithm discern the conversational pairs in an online fashion, without understanding the content of the communications? Our analysis ...

Keywords: Binary time-series clustering, Conversation pairing, Stream clustering, Voice-over-IP

7 [Information security issues in an APL application](#)



[Bill Hillman](#)

June 1984 **APL '84: Proceedings of the international conference on APL**

Publisher: ACM

Full text available: [PDF](#) (549.98 KB)

[Additional Information: full citation, abstract, references, index terms](#)

Bibliometrics: Downloads (6 Weeks): 12, Downloads (12 Months): 24, Downloads (Overall): 258, Citation Count: 0

This paper will describe various methods to secure an APL database application. Primary foci will be in the areas of "physical" protection, and in cryptographic techniques. To that end, distinctions will be made between "data," ...

Also published in:

June 1984 **SIGAPL APL Quote Quad** Volume 14 Issue 4

8 [ACM SIGSAM Bulletin: Volume 39 Issue 1](#)



March 2005

SIGSAM Bulletin





Publisher: ACM

[Additional Information: full citation, index terms](#)

Bibliometrics: Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Downloads (Overall): n/a, Citation Count: 0

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2010 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  [Adobe Acrobat](#)  [QuickTime](#)  [Windows Media Player](#)  [Real Player](#)